AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1   1.   (Previously presented) A method for confirming communication of
2   data to a first device belonging to a first user from a second device belonging to a
3   second user, the method comprising:
4   receiving a message containing data from the second device at the first
5   device;
6   translating the data into a string of dictionary words that can be recognized
7   by a human;
8   allowing the second device to translate the data into a corresponding string
9   of dictionary words;
10   displaying the string of dictionary words to the first user; and
11   allowing the first user and the second user to confirm a match between the
12   string of dictionary words from the first device and the corresponding string of
13   dictionary words from the second device, wherein the confirmation process is
14   performed through a separate communication channel, and wherein the
15   confirmation ensures that the data sent by the second device is successfully
16   received by the first device, is authentic, and is integrity-checked.

1   2.   (Original) The method of claim 1, wherein prior to receiving the
2   message, the first device broadcasts a request asking for the second device's data,
3   and wherein the data can be an identifier.

1   3.   (Original) The method of claim 1,

2   wherein the message received by the first device is signed with a private

3 key corresponding to a public key associated with the second device; and

4   wherein the method further comprises using the public key associated with

5 the second device to verify that the message is signed with the private key

6 associated with the second device.

1   4.   (Previously presented) The method of claim 1,

2   wherein while receiving the message, the first device receives more than

3 one message; and

4   wherein the method further comprises translating the data in the other

5 messages into strings of dictionary words which can be recognized by a human,

6 and displaying these strings of dictionary words to the first user, thereby allowing

7 the first user to match one of these strings of dictionary words with the

8 corresponding string derived by the second device from the original data.

1   5.   (Original) The method of claim 1, wherein prior to the reception of

2 the message at the first device, the first user obtains a portion of the hash of the

3 data on a separate communication channel and enters this portion into the first

4 device, and wherein the first device uses this portion to filter subsequently

5 received messages.

1   6.   (Original) The method of claim 1, wherein the data received at the

2 first device contains a cryptographically generated address (CGA) belonging to

3 the second device, which is generated by:

4   performing a hash function on the second device's public key; and

5   constructing the CGA by combining a number of bits of an address

6 belonging to the second device and a number of bits from the result of the hash

7 function.

1   7.   (Previously presented) The method of claim 6,

2   wherein the message received by the first device includes a public key

3   associated with the second device; and

4   wherein the method further comprises performing a hash function on the

5   public key to verify the association between the CGA and the public key

6   associated with the second device.

1   8.   (Original) The method of claim 1, wherein the translation uses a

2   one-time password (OTP) dictionary.

1   9.   (Previously presented) The method of claim 2,

2   wherein the request includes a Crypto-Based Identifier (CBID) belonging

3   to the first device; and

4   wherein the request is signed with a private key associated with the first

5   device, thereby allowing the request to be verifiably associated with the first

6   device.

1   10.   (Previously presented) A computer-readable storage medium

2   storing instructions that when executed by a computer cause the computer to

3   perform a method for confirming communication of data to a first device

4   belonging to a first user from a second device belonging to a second user, the

5   method comprising:

6   receiving a message containing data from the second device at the first

7   device;

8   translating the data into a string of dictionary words that can be recognized

9   by a human;

10   allowing the second device to translate the data into a corresponding string

11   of dictionary words;

12   displaying the string of dictionary words to the first user; and

4

13   allowing the first user and the second user to confirm a match between the

14   string of dictionary words from the first device and the corresponding string of

15   dictionary words from the second device, wherein the confirmation process is

16   performed through a separate communication channel, and wherein the

17   confirmation ensures that the data sent by the second device is successfully

18   received by the first device, is authentic, and is integrity-checked.

1   11.   (Original) The computer-readable storage medium of claim 10,

2   wherein prior to receiving the message, wherein prior to receiving the message,

3   the first device broadcasts a request asking for the second device's data, and

4   wherein the data can be an identifier.

1   12.   (Original) The computer-readable storage medium of claim 10,

2   wherein the message received by the first device is signed with a private

3   key corresponding to a public key associated with the second device; and

4   wherein the method further comprises using the public key associated with

5   the second device to verify that the message is signed with the private key

6   associated with the second device.

1   13.   (Previously presented) The computer-readable storage medium of

2   claim 10,

3   wherein while receiving the message, the first device receives more than

4   one message; and

5   wherein the method further comprises translating the data in the other

6   messages into strings of dictionary words which can be recognized by a human,

7   and displaying these strings of dictionary words to the first user, thereby allowing

8   the first user to match one of these strings of dictionary words with the

9   corresponding string derived by the second device from the original data.

1   14.   (Original) The computer-readable storage medium of claim 10,

2   wherein prior to the reception of the message at the first device, the first user

3   obtains a portion of the hash of the data on a separate communication channel and

4   enters this portion into the first device, and wherein the first device uses this

5   portion to filter subsequently received messages.

1   15.   (Original) The computer-readable storage medium of claim 10,

2   wherein the data received at the first device contains a cryptographically generated

3   address (CGA) belonging to the second device, which is generated by:

4   performing a hash function on the second device's public key; and

5   constructing the CGA by combining a number of bits of an address

6   belonging to the second device and a number of bits from the result of the hash

7   function.

1   16.   (Previously presented) The computer-readable storage medium of

2   claim 15,

3   wherein the message received by the first device includes a public key

4   associated with the second device; and

5   wherein the method further comprises performing a hash function on the

6   public key to verify the association between the CGA and the public key

7   associated with the second device.

1   17.   (Original) The computer-readable storage medium of claim 10,

2   wherein the translation uses a one-time password (OTP) dictionary.

1   18.   (Previously presented) The method of claim 11,

2   wherein the request includes a Crypto-Based Identifier (CBID) belonging

3   to the first device; and

4   wherein the request is signed with a private key associated with the first

5   device, thereby allowing the request to be verifiably associated with the first

6   device.

1   19.   (Previously presented) An apparatus that confirms communication

2   of data between a first user and a second user, comprising:

3   a receiving mechanism in a first device belonging to the first user, the

4   receiving mechanism configured to receive a message containing data from a

5   second device belonging to the second user;

6   a translation mechanism in the first device configured to translate the data

7   into a string of dictionary words that can be recognized by a human;

8   a display mechanism configured to display the string of dictionary words

9   to the first user; and

10   a confirmation mechanism that allows the first user and the second user to

11   confirm a match between the string of dictionary words from the first device and a

12   corresponding string of dictionary words translated from the data at the second

13   device, wherein the confirmation process is performed through a separate

14   communication channel, and wherein the confirmation ensures that the data sent

15   by the second device is successfully received by the first device, is authentic, and

16   is integrity-checked.

1   20.   (Original) The apparatus of claim 19, wherein prior to receiving the

2   message, the first device is configured to broadcast a request asking for the second

3   device's data, and wherein the data can be an identifier.

1   21.   (Original) The apparatus of claim 19,

2   wherein the message received by the first device is signed with a private

3   key corresponding to a public key associated with the second device; and

7

4   wherein the apparatus further comprises a verification mechanism

5   configured to use the public key associated with the second device to verify that

6   the message is signed with the private key associated with the second device.

1   22.   (Previously presented) The apparatus of claim 19,

2   wherein the first device is configured to receive more than one message

3   while receiving the message;

4   wherein the translation mechanism is further configured to translate the

5   data in the other messages into strings of dictionary words which can be

6   recognized by a human; and

7   wherein the display mechanism is further configured to display these

8   strings of dictionary words to the first user, thereby allowing the first user to

9   match these string of dictionary words with the corresponding string derived by

10 the second device from the original data.

1   23.   (Original) The apparatus of claim 19, wherein prior to the

2   reception of the message at the first device, the first device is configured to enable

3   the first user to obtain a portion of the hash of the data on a separate

4   communication channel and to enter this portion into the first device, and wherein

5   the first device is configured to use this portion to filter subsequently received

6   messages.

1   24.   (Original) The apparatus of claim 19, wherein the data received at

2   the first device contains a cryptographically generated address (CGA) belonging

3   to the second device, which is generated by:

4   performing a hash function on the second device's public key; and

5   constructing the CGA by combining a number of bits of an address

6   belonging to the second device and a number of bits from the result of the hash

7   function.

1   25.   (Previously presented) The apparatus of claim 24,

2   wherein the message received by the first device includes a public key

3 associated with the second device; and

4   wherein the apparatus further comprises a verification mechanism

5 configured to perform a hash function on the public key to verify the association

6 between the CGA and the public key associated with the second device.

1   26.   (Original) The apparatus of claim 19, wherein the translation

2 mechanism uses a one-time password (OTP) dictionary.

1   27.   (Previously presented) The apparatus of claim 20,

2   wherein the request includes a Crypto-Based Identifier (CBID) belonging

3 to the first device; and

4   wherein the request is signed with a private key associated with the first

5 device, thereby allowing the request to be verifiably associated with the first

6 device.